

2024

电子网络安全

关注网络安全 防止网络诈骗 安全上网



制作人:高超

单位: 东营市河口区湖滨新区幼儿园



前 言

“互联网+”的时代改变了人们的生活习惯和行为模式——购物交易、社交娱乐、学习工作，方方面面的需求都可以通过互联网来完成。

我们要如何维护自身的？

目 录

第一部分

国家网络宣传周介绍

第二部分

电脑上网的安全

第三部分

手机上网安全

第四部分

网络购物安全防范

第五部分

常见网络诈骗手法及防范

第六部分

日常网络陷阱防范

第七部分

防骗指南



第一部分

国家网络宣传周介绍



国家网络宣传周介绍

国家网络安全宣传周

即“中国国家网络安全宣传周”是为了“共建网络安全，共享网络文明”而开展的主题活动，围绕金融、电信、电子政务、电子商务等重点领域和行业网络安全问题，针对社会公众关注的热点问题，举办网络安全体验展等系列主题宣传活动，营造网络安全

人人有责、人人参与的良好氛围。





国家网络安全宣传周介绍

2023年国家网络安全宣传周于2023年9月11日至17日举行



2023活动主题

“网络安全为人民 网络安全靠人民”

第二部分

电脑上网安全

网络的正向特点

网络多媒体化的信息，吸引和感染着充满娱乐精神和追求新鲜刺激的人们。

网络广泛的传播面，开阔了视野，丰富了生活，满足了人们渴望广泛关注和被关注的心理。

网络不断增强的互动性，吸引和刺激着思想和行为活跃的人们。

网络极强的时效性，吸引着人们追求新知、了解前沿、知晓新闻的注意力。

网络可以成为人们终身的学习工具。

网络的正向特点



网络的负向特点

网络的开放性与多元性，使人们面临着多元文化思潮和价值观念的影响。

网络的隐匿性和不确定性，使人们面临着被欺骗、被诱导、被利用的危险环境。

网络的不安全性与不可控性，使人们的名誉乃至人身财产安全存在潜在危险。

网络的虚拟性与无约束性，使部分人借此脱离或逃避现实社会所应遵守的规则，沉溺于虚拟世界不能自拔，人的社会属性和社会功能退化。

网络的自主性与平等性，顺应了人们追求个性的心理，使更多地沉浸在自我世界里，缺少对别人的理解尊重。

01

02

03

04

05





网上上网的安全

账号密码安全

- 在网上网过程中，无论是登录网站、电子邮件或者应用程序等等，帐号和密码是用户最重要的身份信息，因此帐号和密码的安全至关重要，一旦丢失会造成严重后果。在注册和使用的过程中应注意：
- 密码的设定一定要科学严谨，不可过于简单，尽量使用字母和数字相结合，具有一定长度的密码。
- 个人帐号和密码信息不可泄漏给他人。
- 在网吧等公用计算机上使用时切勿开启“记住密码”选项，使用完毕后应安全退出，重新启动电脑。



网上上网的安全

账号密码安全

- 设置浏览器的安全等级。
- 我们常用的浏览器都具有安全等级设置功能，通过合理地设置可以有效过滤一些非法网站的访问限制，从而减少对电脑和个人信息的损害。
- 坚决抵制反动、色情、暴力网站。
- 一方面这些不良信息会影响青少年的身心健康，
- 另一方面很多非法网站会利用浏览器漏洞对用户进行各种攻击。
- 不要随意点击非法链接。
- 下载软件和资料时应选择正规网站或官方网站。

第三部分

手机上网安全



手机上网安全

手机上网的基本注意事项

- 关闭常用通讯软件中的一些敏感功能。如微信里的附近的人 微信隐私里“允许陌生人查看照片”等。
- 不能随便晒家人及住址照片。长期这样下去，只要经过别人稍加分析汇总，你所晒出来的信息就会成为一套完整的信息，这就暗藏着各种不可预测的风险。
- 不要随便在网上测试相关信息。有的网站搞调查，问你的年龄、爱好、性别等等信息，你若为了一点小利益去做的话，这些信息就可能被人家利用起来，将你的信息逐渐总结，卖给别人盈利或威胁到你。
- 不要随意扔掉或卖掉旧手机。尤其是那些涉密的旧手机，可能出了些毛病你就打算卖掉或扔掉。千万不要这样，一些人就可以恢复你的数据，这其中暗藏着各种危害，你是无法预测到的。



手机上网安全

手机上网的基本注意事项

- 软件安装过程中不要都“允许”。尤其现在使用的智能手机，安装软件过程中，有的软件提示你是否允许安装全部服务，比如获取你的位置，读取你的电话记录等等，这种情况下，要千万小心，不相关的服务不能允许，或者不安装此软件。
- 不要随便接入公共WIFI。公共WIFI中有些是黑客获取你手机信息的一个重要渠道，可能直接盗取你的敏感信息，如卡号、账户密码等。所以，到公众场合后，有免费WIFI也不要随意接入。
- 不要随意发给别人验证码。验证码可以说是保密的一道重要防线，一旦突破了，那么可能就会有很大的后果等着你。

第四部分

网络交易安全防范

网络交易的类型

01

网购服装。

02

网购日用品、学习用品。

03

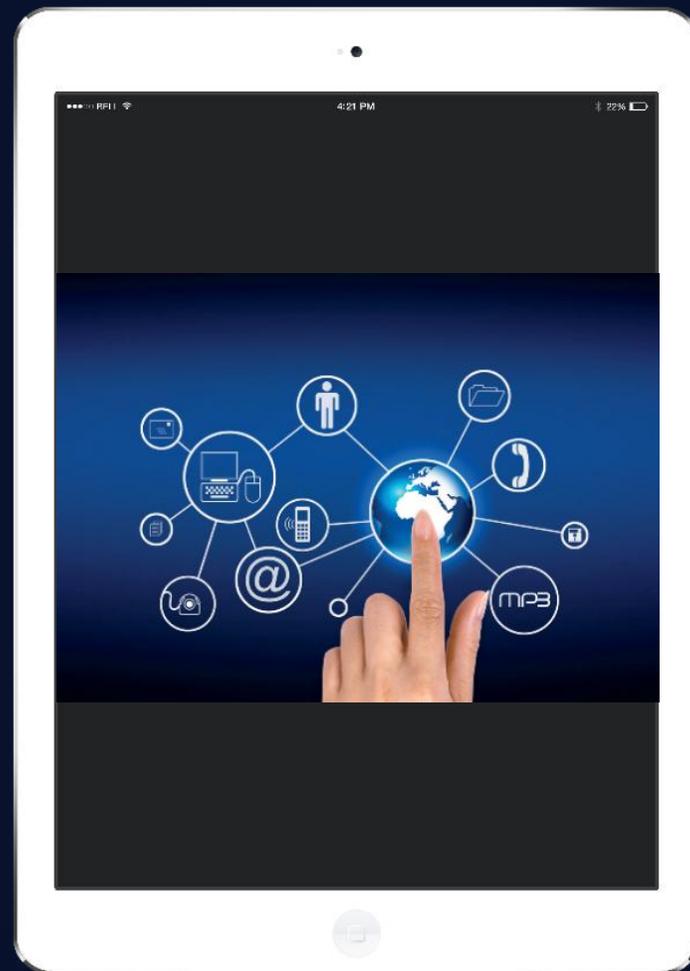
购买电子产品。

04

网上充话费、订机票、订酒店、买彩票。

05

买保险、外出旅游等。



网络交易的特点

网络交易是通过网络信息媒介进行的买卖交易，具有网络信息的鲜明特征，归纳起来，主要有以下几个显著特点：



风险性

消费者在网络交易过程中见不到实物，只能通过商品图片及相关视频资料的描述来了解相关信息，如果缺乏网购经验，在进行网络交易时存在被卖家欺骗的可能性。



隐蔽性

网络交易的整个过程买卖双方并不见面，交易的证据是具有很强隐蔽性的电子证据，如若商家缺失诚信，电子证据容易被删除、修改、屏蔽等，给取证工作带来很大难度，故而网络交易存在比较隐蔽的消极一面。



时效性

网络的一大优势就是速度优势，网络交易的时效性非常强，对于商家来说，商品信息一经发布，即可被世界各地的消费者浏览到；对于消费者来说，只要按照操作步骤轻点鼠标即可完成网络交易。



全面性

网络交易的类型齐全，不仅有品种齐全的有形物品，如服装、生活用品、日用品等，还有为人们生活提供便利的服务项目，诸如网上交费等。



广泛性

网络交易不受地域和时间的限制，通过网络搜索引擎，就可以搜索到自己想要的商品信息，通过网络实时聊天工具，可以用文字、语音或视频面对面和商家进行交流，充分显示出了网络交易的一大魅力。

网络交易的安全防范

01

加强对计算机的防病毒措施，保障网购的安全环境

网络木马病毒是网上银行、支付宝账户等网购支付系统最大的潜在威胁，一旦电脑感染木马病毒，不法分子就会通过木马病毒程序窃取到电脑里的重要信息，甚至可以远程窥探到被害人正在实施的网路行为，进而将网上银行、支付宝、电子游戏等的账号、密码盗取，瞬间转走账户里的资金，使被害人遭受重大的经济损失。

02

谨慎选择电子商务网站，不让钓鱼网站有机可乘

钓鱼网站以假乱真，冒充正规网站欺骗消费者，已经成为了网购一族潜在的又一巨大安全威胁。钓鱼网站看起来与正规合法注册的购物网站没有什么区别，店铺物品琳琅满目，手续齐全，购物流程相似，极具伪装性；但是细细研究却经不起推敲，钓鱼网站往往搞一些促销活动吸引眼球，促销价格比正常价格低得离谱，信誓旦旦保证没有一家同类店铺能比得过它，承诺假一赔十，辅以一些虚假的证书等蒙蔽消费者，最终使消费者上当受骗。

03

谨言慎行，预防新型的诈骗陷阱

网上交易的骗子手段不断翻新花样，不法分子通过发送带有木马病毒的信息到模仿银行、淘宝等知名电子网站，通过高仿真冒充合法站点以及抓住人们对知名网站的信赖心理来迷惑消费者，从而成功实施诈骗。

网络交易的安全防范

选择安全合理的网络交易手段

一般来说，正规的、成熟的、消费者口碑好的商家都支持货到付款，如果碰到先付款再发货的商家或者要求预付保证金，消费者要引起足够警惕，如果对方是知名网站，如航空公司、知名的专业销售网站和网上直营店经过核实后消费者可以通过网银或者邮局先进行付款；但如果是信誉度不高又不是非常知名的网站，尽量避免直接汇现金或转账支付，最好是坚持要求货到付款，检查后发现没有质量问题再支付，避免上当受骗。

04

谨防手机网络诈骗

在网络诈骗之外，一些不法分子更是瞄准了手机网络这个亟待开发的领域，近年来，手机诈骗短信花样繁多，严重损害了人民群众的利益，现就比较典型的案例介绍如下：

05

养成保护网络交易电子证据的好习惯，努力维护好自身的合法权益

网络交易都是在电子信息交换的基础上完成，没有传统媒介真实的纸质证据，电子商务的一些潜在风险使网络交易呈现出了取证难、鉴定难的情况，如果不注意电子证据的保存，电子信息很容易被篡改或丢失，如若出现了交易纠纷，就很难维护消费者的权益。因此，为了自身的网络交易安全，维护好自身的合法权益，买家在完成交易后，应当保存相关电子交易的记录信息，一旦发生商品纠纷进行退换货时，可以向维权单位和部门提出维权申请，有效保护自己的切身利益。

06



网络购物安全防范

购买前要留意商家信誉

确定购买之前，一定要先了解一下卖家的信誉度。卖家的信用评价是一个重要的参考标准。要注意选择合法的网站和商家，一般正规网站都应标注网上销售的经营许可证号和工商机关红盾检验标志。而且，网站应当持有ICP证书，消费者可通过查看网站首页最下方商家的数字证书来验证其“身份”。

不要被低价商品迷惑

特别是名牌产品，因为知名品牌产品除了二手货或次品货，正规渠道进货的名牌是不可能和市场价相差那么远的。

小心商家的文字游戏

当遇到字意模棱两可的介绍时，一定要向卖家询问清楚，以防有些不良卖家玩文字游戏。



网络购物安全防范

最好通过第三方支付

网上购物最好通过安全可靠的第三方交易平台来实现，尽量选择货到付款或交易平台提供的诸如支付宝等带有第三方保障功能的支付方式。同时，使用银行卡进行网络支付时，千万注意不要在网吧电脑等公共设备上使用；最好有专用账户或专用卡作网上支付用，并且卡内不要放太多的现金。如发现问题，及时与银行联系。

邮费太高要小心

购买之前，要跟卖家事先做好沟通，因为地域的关系邮费通常和所标价格不同，以防卖家把商品的价格订得很低，但是邮费却很高。

保存原始证据

对于价格比较高的大宗货品，最好不要在网上购买。如果一定要买的话，则应该向卖家问清来路，并最好要求其开具发票。无论商品价格是否昂贵，消费者都应注意保存和卖家之间的往来邮件、聊天记录，以为日后维权留下证据。

第五部分

常见网络诈骗手法及防范



常见网络诈骗手法及防范

冒充即时通讯好友借钱

骗子使用黑客程序破解用户密码,然后张冠李戴冒名顶替向事主的聊天好友借钱,如果对方没有识别很容易上当.大家如果遇到类似情况最好先与朋友通过打电话等途径取得联系,防止被骗。

网络游戏装备及游戏币交易进行诈骗

常见的诈骗方式一是低价销售游戏装备,在骗取玩家信任后,让玩家通过线下银行汇款的方式,待得到钱款后即食言,不予交易;二是在游戏论坛上发表提供代练,待得到玩家提供的汇款及游戏账号后,代练一两天后连同账号一起侵吞;三是在交易账号时,虽提供了比较详细的资料,待玩家交易结束玩了几天后,账号就被盗了过去,造成经济损失。





常见网络诈骗手法及防范

交友诈骗

犯罪分子利用网站以交友的名义与事主初步建立感情，然后以缺钱等名义让事主为其汇款，最终失去联系。

网上中奖诈骗

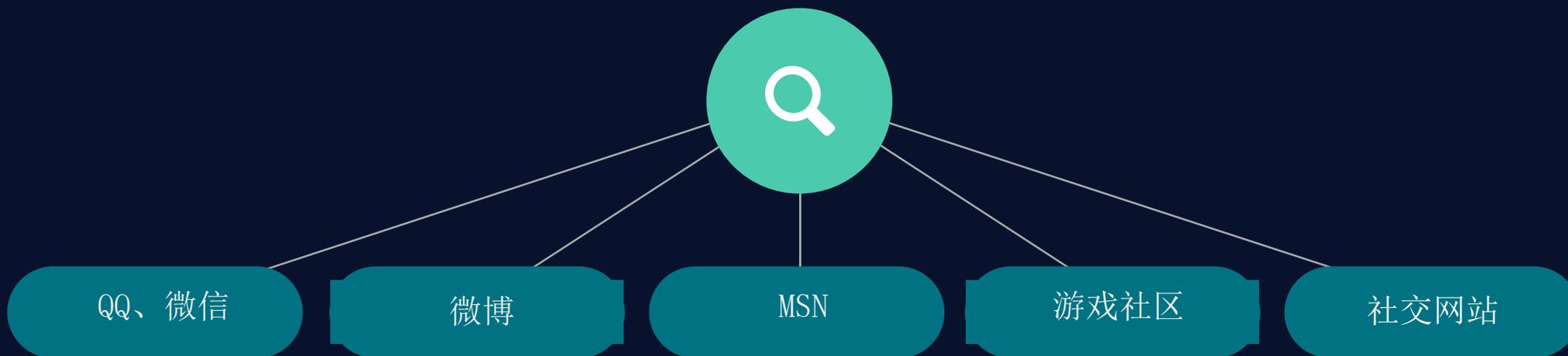
是指犯罪分子利用传播软件随意向手机用户、邮箱用户、即时通讯用户等发布中奖提示信息，当用户按照指定的“电话”或“网页”进行咨询查证时，犯罪分子会以中奖缴税等各种理由让用户一次次汇款，直到失去联系。当收到一些来历不明的中奖提示，不管内容有多么逼真诱人，请大家千万不能相信。

‘钓鱼网站’诈骗

是利用欺骗性的电子邮件和伪造的银行、金融机构网站进行诈骗活动，获得受骗者个人帐户信息进而窃取资金。因此，在访问此类邮件和网站时一定要仔细甄别，认真核实，切勿着急操作。

网络交友的方式

在形式众多的网络交友方式中，主要有以下几类：



网络交友 安全隐患

尽管犯罪分子网上行骗的手法多样，但无论哪种诈骗手法，都有基本固定的一套诈骗方式：他们往往会在一些交友网站或QQ、微信等聊天网站上瞄准一些经济条件较好的女性或个性签名有明显的交友、失恋词语的女性作为目标，进行跟帖或聊天，并投其所好，出手大方，瓦解受害人的戒心。在一系列铺垫行为成功后，犯罪分子便开始为自己编造一些生意遇到困难、投资股票被套牢、买房需要交首付等借口，骗取被害人财物，然后逃之夭夭。有些犯罪分子在行骗不成的情况下，还有可能会出现如绑架等极端行为。因此，在网络交友时，要保持良好心态，学会自我保护。对个人的银行密码、生日、家庭住址、家庭经济状况等隐私，要保密，不可轻易告诉陌生人，更不要和网友发生借贷关系。

1、动机不良，博取信任

2、假借名义，骗钱骗色

网络交友中，动机不良的陌生人往往会将个人信息描述得十分优秀，应谨慎选择交往对象，沟通之前首先查看对方资料，并想办法进行求证，可先在各大搜索网站进行相关查询，一般怀有不良交友动机者，会在很多地方留下此类联系方式，不要急着与之见面。

增强安全意识，提高防范技巧

提高防范技巧，一定要把以下四个步骤记牢。

第一步

保守自己隐私

第二步

提高警惕，留心观察

第三步

不与网友发生金钱交易

第四步

控制约会的时间、地点和尺度



1、保守自己隐私

为了自己的安全，保守个人隐私最为重要。请不要把自己的真实姓名、家庭住址、联系方式、银行卡号等能够让别人直接找到你的信息放到网络上。在注册一些网站或发布网络信息时，除了网站要求公开的基本个人信息外，请尽量少泄漏隐私信息。

具体而言，保守自己隐私的标准就是



**不要把自己真实的信息发布在
网络里**

2、提高警惕，留心观察

对陌生人的网上交友请求，不论对方是同性或异性、出于何种理由，都要时刻保持一颗戒备之心。心怀不轨的人，往往不会有耐心与你慢慢沟通、交流。如果是骗子，一般都会在认识不久就提出见面、视频或与金钱有关的一些要求，要明白结交朋友是需要一个过程的，特别是网友，路遥方知马力。

3、不与网友发生金钱交易

建议不论金钱涉及多少，都不要与网友发生经济上的借贷关系，避免不必要的麻烦。有些骗子会事先给一点甜头，让对方相信他是很大方很讲义气的人，然后施以骗局；还有些骗子只借很少一点钱，或是让帮忙充几十元的电话费，一旦发现是个骗局，往往因为涉及金额不高，也就不再追究，让骗子钻了空子。因此，在任何情况下都不要与网友发生金钱上的往来，如果真的不可避免时，请留下借贷的字据，以备不时之需。

4、控制约会的时间、地点和尺度

如果对网友不是很了解请尽量避免与网友会面。如果感觉时机成熟可以见面时，无论是首次见面还是随后的约会，都要将约会的时间、地点和场所的主动权握在自己的手里。

随着生活方式的转变和生活节奏的加快，现代人交友的方式和途径大别于以前，网络交友作为新的交友方式，务必要提高防范意识、保护个人隐私、把握交友尺度。

具体而言，增强安全知识，提高防范技巧的具体要求就是

保护个人隐私，把握交友尺寸

第六部分

日常网络陷阱防范



日常网络陷阱防范



使用手机APP要谨慎

现在恶意APP程序越来越多，各类非官方下载渠道常被恶意应用。手机用户不使用来历不明的APP，使用正规渠道下载，安装时要注意“应用权限”与产品功能是否直接相关。使用防病毒软件，为手机安全加上防护网站。

手机越狱和root要慎重

安卓root和苹果越狱会带来便利，可以安装更多软件，实现更多高级功能。但如果安装到恶意APP，可以读写删除手机文件、监听截取手机短信等。建议：非专业人员切勿越狱或root，要在官方市场下载应用。





日常网络陷阱防范



陌生人发微信 红包勿乱点

不法分子将手机病毒伪装成微信红包诱导消费者领取，遇到陌生人发送“红包”不要乱点，很可能带有病毒。建议：如果开红包需要填写个人信息等，肯定是骗局，要第一时间关闭手机网络，修改网银、支付宝等密码，然后通过正规途径删除病毒。

摄像头攻击多留心

家庭摄像头已成黑客攻击对象，很可能导致个人隐私泄露等。建议：不要使用预设密码，重置密码越复杂好，需定期更换，摄像头不要对着较私密空间，浴室、床等应置要尽量躲开，在家时可以关闭摄像头电源或用遮挡物挡住。





日常网络陷阱防范



免费打印照片有危害

照片打印成为部分商家“吸粉”利器，且很容易泄露用户信息，比如，扫描二维码可能会让手机感染病毒·建议千万不要见码就扫。

人脸识别也危险

在之前央视315晚会上，人脸识别技术曾被曝出安全隐患，仅凭两部手机、一张随机正面照和一个换脸APP，就能通过3D脸模骗过人脸识别系统。建议：在这技术还没有纯熟之前，慎重使用！





日常网络陷阱防范



智能密码门锁存威胁

技术人员研究发现，现在可以通过之前编写好的破解程序，利用用户注册门锁的手机号码进行破解·建议：最好使用不太常用的手机号码注册，不要把门锁手机号码轻易给不熟悉的人

虚假二维码很可怕

不法分子通过虚假伪装一个网站生成二维码，在受害者扫描二维码时，通过云端软件获取当事人账号、密码等。建议：再重复一遍，千万不要见码就扫



第七部分

防范指南



五 “不”

不轻信

免费了、中奖了、秒杀了、抢红包了、日赚500了... “所有利益诱导性信息都不要轻易理睬；我是领导、我是房东、我是公安、我是老同学、猜猜我是谁、所有装熟人的都不要轻易相信。

不回拨

客服咨询、详情请拨、专属通道——陌生信息中提供的联系方式，都不要轻易致电联系。

不点击

免费领奖、视频相册、工作资料、低价抢购、升级下载、积分兑换。一、、只要是陌生网址，都不要点击。

不透露

手机号码、家庭住址、电子邮箱、亲属联系方式、身份证号、银行卡账号密码、网银登录支付密码、支付宝密码等一切个人以及亲友隐私信息通通不可泄露。

不转账

房补、车补、中奖、退税、银行卡积分兑换现金等不要贪，身份不核实清楚不转账。



核实

核实转账请求

他人要求借钱、打款、线上支付、充值等，所有现金往来一定要当面或电话联系本人确认。

核实转账请求

陌生可疑的短信、电话、QQ、微信、邮件、通知等，只要拿不准情况，都通过线下营业厅、官方网站等官方渠道核实。



养成七个好习惯

- ① 保护好个人身份址和银行卡信息，保存好不用的复印件、交易流水信息
- ② 网上银行操作时，最好手工输入银行官方网站
- ③ 开通账户动账通知短信，发现账户资金异动，立刻冻结或挂失
- ④ 在取款输入密码时用手遮挡
- ⑤ 密码要设置地相对复杂、独立，要定期更换
- ⑥ 进行网上银行、支付账户操作时，不要随意连接不明公共WiFi
- ⑦ 单独设立小额度银行账户，用于日常网上购物等消费



结束语

网络安全与我们的日常生活息息相关

网络隐患无处不在，在使用过程中同学们一定要提高警惕

树立正确的网络安全观念，加强防范意识，减少不必要的损失。

感谢聆听!

